#BuhayPinoyKaalamangPinoy Article 5

'Philippines 2nd most attacked by web threats worldwide last year'

Rainier Allan Ronda - The Philippine Star
March 15, 2023 | 12:00am

MANILA, Philippines — The Philippines was the second most-attacked country by web threats worldwide last year, according to a global cyber security firm's online security monitoring.

Data from the Kaspersky Security Network (KSN) revealed that the country moved two places up, ranking second among countries most attacked by web threats within the period from January to December last year.The 2022 global ranking is topped by Mongolia with 51.1 percent of the attacks recorded, followed by the Philippines (49.8 percent), Ukraine (49.6 percent), Greece (49.5 percent) and Belarus (49.1 percent).

The ranking is based on the number of web-based cyberthreats detected and blocked by Kaspersky products.

Based on the report, a single device can frequently be targeted by cyber criminals and subjected to multiple attacks.

Attempts of local malware spread through removable drives such as flash drives dropped from 35,825,044 in 2021 to 25,060,519 last year. This placed the Philippines in the 72nd spot worldwide, two notches down from its 70th ranking a year ago.

Worms and file viruses accounted for a majority of such incidents that were detected and blocked by Kaspersky products in devices of its Filipino customers, according to the KSN report.

It also showed that cyber criminals tried to penetrate systems through attacks via browsers.

The KSN, however, noted that their detected and foiled incidents plunged from 50,544,908 to 39,387,052.

Drive-by downloads and social engineering are the favorite attack methods used by cyber attackers to spread malware on their victims.

A drive-by download attack is when a user visits a website and unintentionally downloads a malicious code while a social engineering attack is when a user downloads malware, but was made to believe that it is a legitimate program.

If a company employee connects to an unsecured WiFi network or visits a non-work-related website, such actions could result in disastrous and costly damage to company data.

"I would always insist for any business that's new or qualifies as a small and medium enterprise to have basic protection from the get-go. Secure the endpoint and then have encryption in place. As you expand, spending on the business and security should be in lockstep.

It's pointless to build a business that is not protected because once you're compromised, it is costly to repair the damage. At the very least, it could look like losing opportunities for your business because of lost customer trust," Chris Connell, Kaspersky managing director for Asia Pacific, said.

"In the Philippines, businesses continue to flourish despite the challenges. We have seen how adversity, such as the COVID-19 pandemic, hastened the digital transformation among local businesses and customers alike. In the same vein, cyber criminals saw it as an opportunity to take advantage of the cyber security weaknesses of those jumping on the digital wave. As the country moves toward sustaining its recovery, I hope Filipino businesses will be as aggressive in protecting their devices and their data as cyber criminals are persistent in preying on them," Connell added.

To help SMBs and mid-range enterprises secure their networks against cyber criminals, Kaspersky has launched in Southeast Asia a more affordable program to provide two years of enterprise-grade endpoint protection through their Kaspersky Endpoint Security for Business, Cloud or Kaspersky Endpoint Detection and Response Optimum, with 24x7 phone support.

https://www.philstar.com/headlines/2023/03/15/2251710/philippines-2nd-most-attacked-web-threats-worldwide-last-year